Department of Homeland Security Daily Open Source Infrastructure Report for 21 March 2006

Current Nationwide Threat Level is ELEVATED — Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- TechWeb News reports two large botnets that control 150,000 compromised computers are hacking into users' online shopping carts to steal credit card numbers, bank account details, and log−on passwords. (See item 9)
- The Associated Press reports airline pilots departing from Miami International Airport are getting tunes from a pirate radio station that sometimes interfere with control tower communications. (See item 13)
- The Associated Press reports some 13.7 million products subject to Food and Drug Administration regulation entered the U.S. in 2005, but only about 75,000 shipments were sampled and tested, thus allowing unsafe imports to cross the border. (See item 28)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *March 20, Associated Press* — **Pentagon speeds up push for coal fuel.** The Pentagon is trying to persuade investors and the energy industry to embrace an 80−year−old technology to turn coal into liquid fuel to power planes, tanks, and other battlefield vehicles. Officials are concerned that political pressure or terrorist acts could cut the flow of oil from the Middle East

or hurricanes or terrorists could destroy U.S. refineries. "We know what the technical challenges are, but we don't see any show−stoppers...There's still a level of uncertainty, but it looks like the technology is mature enough," said William Harrison of the Pentagon's Assured Fuels Initiative. Mike Carey of the Ohio Coal Association says, "We've probably 250 years' worth of coal." The Pentagon began looking at coal in 2001 when Congress earmarked $13 million to investigate the Fischer−Tropsch process in which coal is gasified and then liquefied into fuel. The process promises to produce a cleaner fuel that would be less subject to freezing, thereby reducing transportation costs and easing logistical headaches by enabling the military to use one fuel for all of its airplanes and vehicles.
Source: http://news.cincinnati.com/apps/pbcs.dll/article?AID=/20060319/NEWS01/603190405/−1/CINCI

2. *March 19, Associated Press* — **Illinois coal mining making a comeback.** Illinois is experiencing a comeback of coal, once king throughout central and southern Illinois. Three new mines capable of producing more than nine million tons of coal annually are expected to open this year. Many credit coal's revival to the fossil fuel increasingly being viewed as an alternative to expensive oil and natural gas. Others point to the binge in construction of new coal−fired power plants to satisfy the nation's surging demand for electricity. "The simple answer is: Oil prices make coal so much more competitive...The economics are all on coal," says Joe Angleton of the state Department of Natural Resources' Office of Mines and Minerals. While coal already produces more than half the nation's energy, the Energy Information Administration forecasts that U.S. coal demand will rise about two percent a year over the next two decades. Across the nation, coal can be found under 458,600 square miles and accounts for an estimated 35 percent of the world's usable coal reserves, the largest of any nation, according to the Illinois Clean Coal Institute.
Source: http://www.chron.com/disp/story.mpl/ap/fn/3733893.html

3. *March 18, Associated Press* — **Utility breaks off talks over natural gas terminal in Pennsylvania.** Philadelphia Gas Works (PGW) has broken off talks with Hess LNG about developing a liquefied natural gas terminal on the Delaware River. PGW spokesperson Doug Oliver said the idea was not dead. He said, "We still remain committed to the development of an import terminal." PGW had been negotiating with Hess since July on a project that would have involved using the company's existing storage tanks in the city's Port Richmond section. Last month, City Council, which would have to approve any deal, passed a resolution denouncing the project.
Source: http://www.newsday.com/news/local/wire/newjersey/ny−bc−nj−−pgw−gasterminal0318mar18,0,2588251.story?coll=ny−region−apnew jersey

4. *March 14, Utility Automation & Engineering* — **Electric Power Research Institute unveils future scenarios to guide strategic planning.** The Electric Power Research Institute (EPRI) has recently unveiled four new scenarios designed to give the energy industry's top decision makers a glimpse of the future with a hope to guide critical decisions in the present. The scenarios explore a range of technologies critical to meet future energy needs, given 100 market drivers with a high potential impact on the evolution of the U.S. energy and electric power industries including: fuel prices, environmental policies, and the availability of natural resources. Rather than predict the future, these scenarios intend to serve as planning tools for utility executives to strategically prioritize technological improvements to yield the most

benefit in the future. The specific technical implications of each scenario will now be developed; EPRI plans to publish those this summer.
Source: http://uaelp.pennnet.com/Articles/Article_Display.cfm?ARTICL E_ID=250234&p=22

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

5. *March 21, Airforce Link* — **The Joint Direct Attack Munition to receive upgrades.** Since its debut in 1999, the Joint Direct Attack Munition, or JDAM, has been called upon more than 15,000 times and continues to be used in the global war on terror. JDAM is a tail kit that turns an unguided dumb bomb, already in the warfighter's arsenal, into an accurate smart munition. Even though JDAM is now a staple of America's arsenal, the Direct Attack Systems Group continues to upgrade the weapon and find new ways for the warfighter to use it to their advantage. JDAM will be one of the first weapons in the inventory to be universal armament interface compliant. This technology will allow the Air Force and Navy to incorporate new precision−guided munitions and current weapon upgrades onto its aircraft without major changes to aircraft software −− a process that takes years and is very costly. The jointly manned JDAM Squadron is also working with the Department of the Navy to add a laser seeker to the weapon. Another way the JDAM Squadron is considering making the weapon more useful against moving targets is by adding a data link.
Source: http://www.af.mil/news/story.asp?id=123017613

[Return to top]

Banking and Finance Sector

6. *March 20, TechWeb News* — **Microsoft vows to keep pressure on phishers.** Microsoft on Monday, March 20, promised to file more than 50 new lawsuits against phishing scammers before the middle of the year, its next step in a global campaign to combat Internet criminals. Company officials announced the plans at the debut of what Microsoft calls its Global Phishing Enforcement Initiative, a worldwide effort to coordinate and expand anti−phishing work through prosecution, partnerships, and consumer protection software, such as the beefed−up Internet Explorer 7 browser scheduled to release later this year. By the end of June, Microsoft will have initiated at least 51 new anti−phishing cases in the company's European, Middle Eastern, and African territories, bringing the total filed to over 100. Microsoft claimed that it had shut down nearly 5,000 phishing sites worldwide, and had filed 117 phishing−related lawsuits in the U.S. alone during 2005.
Source: http://www.techweb.com/wire/security/183700984;jsessionid=2O G3VSQZ3IDXIQSNDBCSKHSCJUMEKJVN

7. *March 19, Government Technology* — **Organization calls on Congress to refocus on data security legislation.** The Cyber Security Industry Alliance (CSIA) last week urged Congress to redouble efforts to pass data breach legislation as well as an international cybercrime convention, in the wake of a widespread and growing international rash of compromised debit card and PIN numbers that one analyst has called "the worst hack ever." CSIA Executive Director Paul Kurtz said: "The debit card scam that has hit several major banks provides an example of how computer crime has changed over the past few years...First, it appears that this was perpetrated by organized criminals seeking to steal money anonymously, rather than by individual hackers looking to make trouble for the sake of bragging rights. Second, the bad guys here are operating in multiple countries, making it much more difficult for law enforcement agencies to pursue those outside the U.S...America's consumers, already buffeted by the threat of identity theft, are now confronted with the reality that even personal identification numbers won't protect them or their bank accounts."
Source: http://www.govtech.net/magazine/story.php?id=98821

8. *March 18, Tallahassee Democrat (FL)* — **Hackers create a new scam.** An Internet scam that prompted three area banks to temporarily shut down their Websites is a new scheme designed to get confidential data from unsuspecting customers, officials said Friday, March 17. The Florida Department of Law Enforcement and FBI officials were notified Tuesday, March 14, after hackers obtained access to computers at ElectroNet Inc., a Tallahassee Internet service provider, and were able to redirect bank customers to counterfeit Web pages. The banks involved −− Capital City Bank, Wakulla Bank, and Premier Bank −− closed down their Websites once the scheme was discovered. The sites were back up by Thursday afternoon, March 16. The hackers gained access to the computer hosting the legitimate home pages of the three banks and routed customer inquiries to a bogus page. Customers who clicked on the counterfeit page were sent to another fake page that asked them to provide account information and other sensitive data.
Source: http://www.tallahassee.com/apps/pbcs.dll/article?AID=/20060318/BUSINESS/603180310/1003

9. *March 17, TechWeb News* — **Botnets steal from e−shopping carts.** Two large botnets that control 150,000 compromised computers are hacking into users' online shopping carts to steal credit card numbers, bank account details, and log−on passwords, security company FaceTime said Friday, March 17. The botnets were discovered, probed, and disclosed to authorities with the help of an insider who tipped off the company's security researchers. According to Chris Boyd of FaceTime, the bots, or hacked PCs, were accumulated by seeding Trojan horses via instant messaging networks. Recipients who clicked on the IMs' embedded link ended up with remote access applications secretly installed on their PCs; the attacker then used that software to install additional malware. One, dubbed "Carder," is designed to sniff out exploits in several e−commerce shopping cart applications. If Carder identifies a vulnerability, both personal data can be snatched from the individual PC, and credit card account numbers, usernames, passwords, and home addresses can be hijacked from the e−tailer's back−end systems. It's impossible to know exactly what shopping cart vulnerabilities are under attack since Carder is so customizable.
Source: http://www.techweb.com/article/printableArticle.jhtml;jsessionid=IBGI3PUIJCOWYQSNDBOCKICCJUMEKJVN?articleID=183700661&site_section=700028

10. *March 17, eWeek* — **Visa issues cash−register flaw warning.** The U.S. arm of credit and debit card giant Visa International has issued an alert for flaws in cash−register software made by Fujitsu Transaction Solutions that could put sensitive cardholder information at risk. According to a report in The Wall Street Journal, the bug can cause the inadvertent storage of customer data—including secret PINs—within the point−of−sale software installed in retail locations. The report said Visa USA sent the warning to "merchant acquirers" that process card transactions for some of the biggest names in retail and urged users to apply a software upgrade from Fujitsu to fix the flaw. A Fujitsu spokesperson quoted by the Journal denied the software was being used in data theft attacks and disagreed with Visa's decision to issue the warning. According to a recent research report by Gartner analyst Avivah Litan, retailers in the United States incorrectly store PIN information and data on point−of−sale terminals instead of destroying the data as required by card industry guidelines.
Source: http://www.eweek.com/article2/0,1895,1939301,00.asp

11. *March 16, Associated Press* — **Music Website says breach exposed accounts.** A musical instrument Website notified some customers that their credit card information may have been stolen. The warning, which came more than a month after someone broke into Bananas.com, was delivered Wednesday, March 15. Website operators still are trying to determine how the intruder gained access. Following the discovery, administrators changed passwords and added other safeguards to restrict unauthorized access to the system, Bananas.com owner J.D. Sharp said. The breach was discovered after an individual identified only by the screen name SmookeR advertised in an Internet chat room the sale of compromised credit card information. In late February, SmookeR released the names, addresses, phone numbers, and credit card numbers of at least 31 people who had recently placed orders at the company.
Source: http://crm.ittoolbox.com/news/display.asp?i=140255

[Return to top]

Transportation and Border Security Sector

12. *March 20, Aviation Week* — **Coast Guard, Navy eye uses for unmanned surfaces vehicles.** The Coast Guard is interested in the Navy's force protection−antiterrorism unmanned surface vehicles under development for the Littoral Combat Ship (LCS) mission modules, but nothing formal has been worked out, according to Navy Capt. Walt Wright, program manager for LCS mission modules. Wright, briefing reporters at the Washington Navy Yard on Wednesday, March 15, said he has briefed Coast Guard Adm. Patrick Stillman, program manager for the Department of Homeland Security armed service's massive Deepwater recapitalization effort, on LCS modules. The cross−service interest comes as the Navy and Coast Guard have inked a commitment to earnestly coordinate their acquisitions in similar and complementary missions.
Source: http://www.aviationnow.com/avnow/news/channel_aerospacedaily_story.jsp?id=news/CGL03206.xml

13. *March 20, Associated Press* — **Pirate radio interferes with Miami pilots.** Airline pilots departing from Miami International Airport are getting an earful of something unexpected: Hip−hop tunes from a pirate radio station that sometimes interfere with their communications with the control tower. The music comes on a pair of frequencies from a station that calls itself

Da Streetz. "It's intermittent. Not all day, everyday," said Kathleen Bergen, a Federal Aviation Administration spokesperson. "But clear communication between air control and the pilots is a critical part of flying." Authorities traced the signals to an antenna at a nearby warehouse but did not find the disc jockey, although they did confiscate equipment including three computers and a CD player. Pilots who pick up the broadcasts switch to a different frequency to speak with air traffic controllers, Bergen said.
Source: http://www.usatoday.com/travel/flights/2006−03−19−pirate−rad io_x.htm

14. *March 20, Associated Press* — **Storm wreaks travel havoc on Plains, Texas.** A storm system barreled across the Plains states on the last day of winter, dumping more than a foot of snow that closed hundreds of miles of major highways Monday, March 20, and causing flooding in Texas. Six−foot snowdrifts were reported in northwestern South Dakota. About a 50−mile section of westbound Interstate 80 was closed in western Nebraska, the Nebraska State Patrol said, and Colorado closed eastbound lanes of I−70 from just outside Denver to the Kansas line, a stretch of about 150 miles. Kansas shut down about 25 miles of I−70 near the Colorado line. Two passenger trains were stalled for hours Sunday, March 19, in the Colorado mountains after a separate rail maintenance vehicle derailed because of the storm. The Ski Train, which runs between Denver and the Winter Park resort, was stopped for about five hours with some 700 aboard, and an Amtrak train had to wait behind it.
Source: http://www.southernillinoisan.com/articles/2006/03/20/ap/hea dlines/d8gfg3800.txt

15. *March 20, South Florida Sun−Sentinel* — **Safety board tallies air deaths.** The Chalk's seaplane crash in Miami accounted for the bulk of U.S. airline deaths in 2005, the National Transportation Safety Board said Friday, March 17. In all, 22 people died in three fatal accidents −− including all 20 on board the Chalk's Grumman Mallard, after a wing broke off on December 19. That crash is still under investigation. In the other accidents: A baggage−loader driver was killed when his vehicle rammed a US Airways Express jet at Washington Reagan National Airport in June; and a Southwest Boeing 737 slid off the runway at Chicago Midway and rammed a car, killing a six−year−old boy in December.
Source: http://www.sun−sentinel.com/news/local/palmbeach/sfl−pcsntsb 18mar18,0,2625262.story?coll=sfla−news−palm

[Return to top]

Postal and Shipping Sector

16. *March 20, KOLD News (AZ)* — **Tucson post office evacuated in drill.** The threat of anthrax attacks through the mail is so serious postal officials are taking no chances. Last summer, a biohazard detection system was installed at the Tucson, AZ, mail processing facility as a safeguard. Tuesday, March 14, they conducted Tucson's first biohazard emergency drill in the postal facility. Once the detection system picks up a trace of biohazardous chemicals like anthrax on a piece of mail, the alarm sounds. That prompts workers and customers to evacuate the building as the facility goes into lock−down. During Tuesday's drill, nearly one hundred employees filed outside toward the facility's back lot. There, they took a head count to make sure no one was left behind. If this were a real emergency instead of a drill, the workers would be decontaminated at the scene. "What we have set up over here is one shower system that has male and female rows, they would line up in those things, and as they go through, they would

disrobe their outer clothing, and they would shower off," explained Brad Olson, Emergency Preparedness Chief with the Tucson Fire Department. Then, the workers would receive antibiotics on−site.
Source: http://www.kold.com/Global/story.asp?S=4600369&nav=14RTY3ZV

17. *March 20, DMNews* — **Parcel consolidators fill void after APX files for Chapter 11.** News that third−party logistics provider APX Logistics had filed for Chapter 11 bankruptcy protection left parcel consolidators scrambling to sign up clients. A parcel consolidator can offer shippers deeper discounts from the postal service without the risk of delivery area surcharges. APX is the largest of the dozen or so Parcel Select mailers partnering with the U.S. Postal Service (USPS). Companies save money by mailing sorted parcels closer to their ultimate destination via three levels of entry: bulk mail centers, sectional center facilities, or destination delivery units. A USPS spokesperson said its sales staff is in contact with APX customers who are seeking advice on how to handle their packages. “We are working with them and offering them a postal solution or directing them to an alternative supplier,” USPS spokesperson Gerry McKiernan said. DHL Global Mail has been contacted by several APX customers, said David Marin−kovich, senior vice president of marketing and customer service at DHL Global Mail.
Source: http://www.dmnews.com/cgi−bin/artprevbot.cgi?article_id=3610 8

[Return to top]

Agriculture Sector

18. *March 17, CNN* — **Calf from infected Alabama cow being tested.** One of at least two calves born to an Alabama cow with mad cow disease will be tested for evidence of the disease, the state's agriculture commissioner said Friday, March 17. The cow was at least 10 years old when it was destroyed last week. Its remains have been sent to a government laboratory in Ames, IA, for testing, Alabama Agriculture and Industries Commissioner Ron Sparks said. The location of the other calf, which was born in early 2005, is unknown. The six−week−old calf is in quarantine. It is the third confirmed case of mad cow disease in the U.S. The first appeared in December 2003 in a Canada−born cow in Washington state. The disease was found again in June in a cow that was born and raised in Texas.
Source: http://www.cnn.com/2006/HEALTH/03/17/mad.cow/

[Return to top]

Food Sector

19. *March 20, Agence France−Presse* — **Japan rejects U.S. calls to end beef ban.** Japan has rejected a U.S. call for the immediate resumption of U.S. beef imports. "Unless safety is firmly secured, imports cannot resume," Chief Cabinet Secretary Shinzo Abe, the government spokesperson, told a news conference. "In the first place, Japanese consumers will not buy it" if Washington fails to prove U.S. beef is safe, Abe said. Japan, which had been the largest overseas market for U.S. beef, banned U.S. beef in December 2003 after a mad cow case was discovered in a herd in Washington state. Japan ended the embargo in December 2005. But it

imposed a new ban just one month later after a beef shipment violated Japanese safety guidelines.
Source: http://news.yahoo.com/s/afp/20060320/hl_afp/healthjapanustrademadcow_060320114810;_ylt=Agl6bBuaQgcop3DK8gR3IW2JOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

20. *March 20, USAgNet* — **Man found guilty of violating Ohio's meat inspection law.** The Girard, OH, Municipal Court found a man guilty of violating Ohio's meat inspection law on two counts. Several department investigations found that Guy DePizzo, Jr. of DePizzo Sausage Company, continued to manufacture and sell his sausage and beef jerky products under the state's "Mark of Inspection" after he terminated his license with the state on March 31, 2005. On another count, DePizzo processed the sausage without having a required Hazard Analysis and Critical Control Point plan. The plan is required to identify process hazards, establish critical control points to prevent those hazards from occurring, and establish records to monitor and document the prevention of food safety hazards.
Source: http://www.usagnet.com/story−national.cfm?Id=447&yr=2006

21. *March 20, Associated Press* — **Canadian meat processing plants up to standard.** Japanese officials on Monday, March 20, declared Canadian meat processing plants up to standard following an inspection tour of the country. Japanese officials have now completed their tour of all Canadian facilities exporting to Japan. Eight plants −− five in Alberta, two in Ontario, and one in Saskatchewan −− currently have permission to process Tokyo−bound shipments. Japan imposed a ban on U.S. and Canadian beef imports in 2003 after the first detection of mad cow disease in the countries, and reopened its market in December. Japan has since reimposed its ban on U.S. beef imports.
Source: http://www.cattlenetwork.com/content.asp?contentid=24106

22. *March 17, Agricultural Research Service* — **Rapid Salmonella test may reduce meat and produce recalls.** An innovative test to detect Salmonella in ready−to−eat meats has been developed by Agricultural Research Service (ARS) scientists. The preliminary test −− still being evaluated by agency researchers −− relies on polymerase chain reaction technology to detect food−contaminating microbes on a molecular level. ARS scientists Jitu Patel and Arvind Bhagwat compared their laboratory−developed “molecular beacon” test to a commercial rapid−detection test currently in use. While both tests can detect Salmonella in eight hours, the laboratory test is less expensive than commercial kits. To evaluate the new test's efficacy, the scientists artificially contaminated various meats (turkey, bologna, and ham slices) and produce (mixed salad, sprouts) with S. enterica serovar Typhimurium and allowed it to incubate for 20 hours. Both tests were sensitive enough to detect contamination in the meat products at an estimated level of two to four cells per 25 grams. In comparing the tests after a relatively brief incubation period of eight hours, two to four cells of Salmonella were detected in the 25−gram samples of meat as well as produce.
Source: http://www.ars.usda.gov/is/pr/2006/060317.htm

[Return to top]

Water Sector

23. *March 20, Associated Press* — **Perchloroethylene found in wells.** Pennsylvania environmental authorities will begin drilling wells in Gilbertsville to try to determine where contaminated groundwater is flowing. The Department of Environmental Protection, which plans six monitoring wells, will also try to determine whether exposure to one contaminant is more widespread than previously thought. Past tests indicate that the 17 contaminated private wells in Gilbertsville contain water with concentrations of perchloroethylene that exceed safe standards.
Source: http://abclocal.go.com/wpvi/story?section=local&id=4007193

24. *March 20, University of New York at Buffalo* — **Pharmaceutical metabolites found in wastewater.** University of New York−Buffalo chemists have for the first time identified at wastewater treatment plants the metabolites of two antibiotics and a medical imaging agent. The data will allow wastewater treatment plants to begin monitoring for these byproducts. The results also reinforce concerns about excreted pharmaceutical compounds from wastewater systems that may end up in the water supply. According to Diana Aga, assistant professor of chemistry, it has been only in the past five years that analytical−chemistry techniques have become sufficiently affordable and practical to allow researchers to detect pharmaceuticals and their metabolites efficiently at the parts−per−billion and parts−per−trillion range. "Current wastewater treatment processes are optimized to reduce nitrates and phosphates and dissolved organic carbon, the major pollutants of concern in domestic wastes," said Aga. "However, treatment facilities don't monitor or measure organic microcontaminants like residues of pharmaceuticals and active ingredients of personal care products."
Source: http://www.buffalo.edu/news/fast−execute.cgi/article−page.ht ml?article=78260009

[Return to top]

Public Health Sector

25. *March 20, Associated Press* — **Israel confirms first outbreak of bird flu.** Israel on Monday, March 20, confirmed its first outbreak of the H5N1 strain of bird flu. The Agriculture Ministry said the flu had been found in birds at two communal farms in southern Israel and at a farming community in central Israel. Fearing the worst, Israel had gone ahead Saturday, March 18, with the slaughter of hundreds of thousands of chickens and turkeys. On Sunday, March 19, Egypt reported its second human case of avian flu −− a man who worked on a chicken farm in the province of Qalyoubiya.
Source: http://www.cbsnews.com/stories/2006/03/20/ap/world/mainD8GF4 NPG0.shtml

26. *March 20, Reuters* — **Low−dose flu shots could stretch supply.** Five people can be protected with just one dose of seasonal flu vaccine, researchers said on Monday, March 20. The researchers were able to stretch the supply of vaccine by administering doses one−fifth the normal strength with injections under the skin instead of into muscle, the way full−strength doses are normally delivered. The findings were presented at a meeting of the Society of Healthcare Epidemiology of America. The study vaccinated 1,602 healthy people with a reduced−dose vaccine. It produced similar results as standard doses.
Source: http://today.reuters.com/business/newsArticle.aspx?type=heal th&storyID=nN15412287

27. *March 20, Agence France−Presse* — **Africa plans continental fight against bird flu.** Experts from 46 African nations, the Food and Agriculture Organization, the World Health Organization, and the United Nations Development Program met Monday, March 20, to thrash out an emergency strategy to face a potential bird flu epidemic. The H5N1 bird flu has now been officially detected in poultry in four African countries −− Cameroon, Egypt, Niger, and Nigeria −− while Egypt has reported two suspected human deaths from bird flu. Bird flu poses a particularly worrying threat for Africa, which lacks the basic health care and infrastructure of the developed world, and where poultry and humans tend to live in close proximity.
Source: http://news.yahoo.com/s/afp/20060320/hl_afp/healthfluafrica_060320143554;_ylt=Aj4a_NFrLK2ViaGOybyaIa6JOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

28. *March 19, Associated Press* — **Unsafe imports slip through regulatory net.** The poison arrived in a plastic bottle from India bearing a simple label. "Useful in flu and body ache," it read. "Two tabs twice a day or as per physician's advice." The herbal medicine, on sale at a store in Queens, NY, contained 2,190 times the amount of mercury considered safe. The tablets were among a variety of imported products seized by New York City health officials last year −− some of which make it onto shelves without being evaluated by safety agencies. Some 13.7 million imported products subject to Food and Drug Administration regulation entered the U.S. in 2005, compared to 7.9 million three years earlier. Almost all shipments are subject to automated screening, during which computers hunt cargo invoices for products with potential safety problems −− but only about 75,000 shipments each year wind up being sampled and tested. The system is less effective when it comes to undocumented cargo that crosses the border daily.
Source: http://www.boston.com/yourlife/health/other/articles/2006/03/19/unsafe_imports_slip_through_regulatory_net/

29. *March 16, University of Wisconsin at Madison* — **Scientists reveal how deadly toxin hijacks cells.** Scientists have pinpointed exactly how botulinum neurotoxin A −− a potential agent of biological warfare −− is able to sneak into cells. The finding is crucial for the development of new treatments against botulism, a paralytic illness caused by the toxin more commonly known as botox. A team of researchers at the University of Wisconsin−Madison and the University of Texas report that botox latches onto a protein known as SV2 to gain entry into neurons. "Knowing the protein receptor for [botulinum toxins] can pave the way for developing anti−toxin reagents which may block the entry of toxins into cells," said lead author Min Dong. The botulinum toxins, of which there are seven types, are made by a bacterium commonly found in soil, known as Clostridium botulinum. The toxin enters neurons by binding to nerve endings and preventing the release of crucial chemical messengers, known as neurotransmitters, that communicate with muscles. When enough nerve endings are invaded, botox can lead to paralysis and death.
Source: http://www.news.wisc.edu/12291.html

[Return to top]

Government Sector

Nothing to report.

[Return to top]

Emergency Services Sector

30. *March 20, Huntington News (WV)* — **Second West Virginia Homeland Security Summit conducted.** With 375 participants in attendance, Senator Jay Rockefeller (D−WV) and the State of West Virginia kicked off the 2nd West Virginia Summit on Homeland Security on Sunday, March 19. The two−day Summit, organized by Rockefeller, includes first responders, school officials, scientists, health experts, and government officials. Sunday's activities included a number of demonstration projects led by the West Virginia National Guard, the West Virginia State Police, the U.S. Coast Guard and others that illustrated the state's response capabilities and some of the techniques that emergency officials can employ in the event of an emergency. These demonstrations, which included mass decontamination exercises, bomb detection teams, and waterborne intervention displays, gave participants hands−on experience to cutting−edge technology and tactics.
Source: http://www.huntingtonnews.net/state/060319−staff−security.ht ml

31. *March 19, Radio World Newspaper* — **FCC creates new public safety bureau.** The Federal Communications Commission (FCC) voted to create a Public Safety and Homeland Security Bureau within the agency to help it respond faster to terrorist attacks, natural disasters and other emergencies. Public safety communications, Emergency Alert System, 911 emergency calling rules, disaster management and network security would be handled in the new bureau. The new bureau would be created after congressional notification, according to Tony Dale, Office of the FCC's Managing Director.
Source: http://www.rwonline.com/dailynews/one.php?id=8703

32. *March 18, Associated Press* — **Drill will address language barriers.** Officials in St. Cloud, MN, which has seen an influx of immigrants, are working on plans for relaying information to non−English speaking residents in emergencies. Planning for a tornado drill, slated for May 22, is underway. The objective: to test the county agencies' responses to a crisis affecting non−English speaking populations.
Source: http://www.twincities.com/mld/twincities/news/local/14127470 .htm

[Return to top]

Information Technology and Telecommunications Sector

33. *March 20, Netcraft* — **Bot authors targeting phpBB forums.** A bot by the name of FuntKlakow is registering user accounts on thousands of phpBB forums across the Internet, raising concerns that the bot's authors are laying the groundwork for mass exploitation down the road. FuntKlakow post signatures have included links to proxy surfing and "traffic generator" services, raising the prospect that its goal may be spam rather than exploits.
Source: http://news.netcraft.com/archives/2006/03/20/bot_authors_targeting_phpbb_forums.html

34.

March 20, IDG News Service — **Tough week ahead for 'badware' companies.** The fight against invasive software will take a step forward this week as the Center for Democracy and Technology (CDT) and the Google−backed Stopbadware Coalition will release two separate reports that state the names of undesirable software programs and the advertisers who help fund them. On Monday, March 20, the CDT will publish its report on the major advertisers who are behind so−called "adware" software. Two days later, the Stopbadware Coalition is set to release its first report, which will name several software programs to its Badware Watch List.
Source: http://www.infoworld.com/article/06/03/20/76595_HNbadware_1. html

35. *March 20, CNET News* — **Annual telecommunications conference underway.** As the most influential executives in the telecommunications industry gather this week in Las Vegas for their annual conference, they're more likely to be talking about TV than phones. An all−star lineup of executives −− including Ivan Seidenberg, CEO of Verizon Communications; Edward Whitacre of AT&T; Robert A. Iger, CEO of The Walt Disney Company; Glenn Brit, CEO of Time Warner Cable; and Kevin Martin, Federal Communications Commission chairman −− will be taking the stage at TelecomNext starting Monday afternoon, March 20. Potential conference topics include: regulatory issues, Net neutrality, Internet Protocol TV and wireless communications.
Source: http://news.com.com/Whats+next+in+telecommunications/2100−1037_3−6051317.html?tag=nefd.lede

36. *March 19, Securi Team* — **Microsoft Commerce Server 2002 authentication bypass.** Improper authentication validation allows attackers to authenticate as an existing user in Microsoft Commerce Server 2002. Analysis: The problem is in the sample files of "authfiles." If the user makes his/her own solution site in Commerce Server and the "authfiles" are installed on the server, the user is vulnerable for positive user logon's using false passwords. If someone knows a user (some sites uses an e−mail address) and goes to http://site/authfiles/login.asp (some sites have it in another directory) and enters the Username and a false password, the user will get an error. After the error, if the user goes with the same browser to the root directory of the site, http://site/, another error occurs. Then, if the user navigates again to the site he/she will be logged on as the entered user. Vulnerable Systems: Microsoft Commerce Server 2002. Immune Systems: Microsoft Commerce Server 2002 SP2.
Vendor Status: The vendor has issued a warning:
http://msdn.microsoft.com/library/default.asp?url=/library/en−us/csvr2002/htm/cs_se_securityconcepts_cbgw.asp
The vendor has issued the following fix:
http://www.microsoft.com/downloads/details.aspx?familyid=58e6d658−cc3e−4846−8ef7−264e6eeb4c1e&displaylang=en
Source: http://www.securiteam.com/windowsntfocus/5AP0C2KI0E.html

37. *March 18, FrSIRT* — **HP−UX "usermod" command options local unauthorized access vulnerability.** A vulnerability has been identified in HP−UX, which could be exploited by local attackers to bypass security restrictions and gain unauthorized access to arbitrary files and directories. Analysis: This flaw is due to an error in the "usermod" command when handling certain options, which could be exploited to recursively change the ownership of all directories and files under a user's new home directory and gain unauthorized access to these directories and files. Affected products: HP−UX B.11.00; HP−UX B.11.11; HP−UX B.11.23.

Solution: HP−UX B.11.11 −− Install PHCO_33142.
HP−UX B.11.00 and HP−UX B.11.23 −− Apply workarounds:
http://www2.itrc.hp.com/service/cki/docDisplay.do?docId=c006 14838
Source: http://www.frsirt.com/english/advisories/2006/0997

38. *March 17, eWeek* — **Apple issues updated security fix.** Apple released another version of the security patch it distributed on Monday, March 13, to users of its OS X operating system software, in order to address a problem reported with the update. The company said it distributed the new patch, dubbed Update 2006−002 v1.1, in order to fix an issue with Apple's Safari Web browser that some users observed after installing its 2006−002 security update. According to a post on the company's Website, the flaw specifically affected users who removed Safari from their computers' applications folders before installing the 2006−002 patch.
Source: http://www.eweek.com/article2/0,1895,1939478,00.asp

39. *March 17, IDG News Service* — **New Spycar software will test antispyware.** With security experts warning of "rogue" antispyware products that sometimes do more harm than good, two security researchers have decided to take matters into their own hands. They're working on a new software product, called Spycar, that will test the effectiveness of antispyware products. Spycar will contain about 25 small programs, each of which engages in the kind of nasty behavior normally associated with spyware. The software will then undo all of the changes it has made after the testing has been completed. Spycar will be available free of charge in May. More information will be made available on the http://www.intelguardians.com Website at that time.
Source: http://www.infoworld.com/article/06/03/17/76590_HNspycar_1.h tml

40. *March 16, Macworld* — **Hackers get Intel Mac to run Windows XP.** A contest to see who could get Windows XP working first on an Intel Mac has been won, according to the contest's coordinator, Colin Nederkoorn. Getting Windows XP to work on the Mac is not a plug and play process. According to the documentation included with the file download provided on Nederkoorn's Website, users must create an install CD themselves using a PC equipped with a CD−R drive, Microsoft's Windows XP SP 2 CD−ROM and Nero CD burning software. Step−by−step instructions for creating the disc are included. Users must also reformat and repartition their Intel Mac's hard disk drive to include a separate partition where Windows XP can be installed, then go through a multi−step process to make sure the software is installed properly and the Mac can recognize it. Once that's done, users will be able to switch between Mac OS X and Windows after rebooting the Mac.
To load Windows XP on an Intel Mac: http://onmac.net/
Source: http://www.macworld.com/news/2006/03/16/xponmac/index.php

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is aware of several vulnerabilities in Adobe Macromedia Flash products. A system may be compromised if a user accesses a web page that references a specially crafted Flash (SWF) file. Successful exploitation may allow a remote attacker to execute arbitrary code with the privileges of the user. For more information please review the following:

VU#945060 − Adobe Flash products contain multiple vulnerabilities
http://www.kb.cert.org/vuls/id/945060

TA06−075A − Adobe Macromedia Flash Products Contain Vulnerabilities
http://www.us−cert.gov/cas/techalerts/TA06−075A.html

Adobe Security Bulletin: APSB06−03
http://www.macromedia.com/devnet/security/security_zone/apsb 06−03.html

Microsoft Security Advisory: 916208
http://www.microsoft.com/technet/security/advisory/916208.ms px

US−CERT encourages administrators to apply the appropriate updates, patches, or fixes as soon as possible.

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 25 (smtp), 445 (microsoft−ds), 55620 (−−−), 139 (netbios−ssn), 39972 (−−−), 55556 (−−−), 5435 (dttl), 6881 (bittorrent), 6883 (DeltaSourceDarkStar) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.
[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer